第92124489號初審引證附件2

31例2.

TW479191

中華民國專利公報 [19] [12]

[11]公告編號：479191
[44]中華民國 91年 (2002) 03月11日
發明 全15頁
[51] Int.Cl [07]： G06F7/00

[54]名 稱：相互認證方法，記錄裝置，再生裝置，和記錄媒體

[21]申請案號： 089111880 [22]申請日期：中華民國 89年 (2000) 06月16日
[30]優 先 權： [31]11-170187 [32]1999/06/16 [33]日本

[72]發 明 人：
上林遜 日本
山田尚志 日本
岩崎博 日本
田村正文 日本
石橋泰博 日本
加藤拓 日本
館林誠 日本
原田俊治 日本
[71]申 請 人：
東芝股份有限公司 日本
松下電器產業股份有限公司 日本
[74]代 理 人： 林志剛 先生

[57]申請專利範圍：

1.一種用於對記錄媒體上複製的內容進行記錄之記錄裝置與該記錄媒體之間的相互認證方法，該記錄媒體具有算術處理功能，該方法包括下列步驟：

至少將取決於該記錄媒體的第一筆資訊儲存於該記錄媒體中，而亦取決於該記錄媒體的第二筆資訊將於與該記錄裝置執行相互認證時，與該記錄裝置共享；及

由該記錄裝置產生認證資訊，其用於依據得自於該記錄媒體之第一筆資訊而與該記錄媒體進行相互認證，並使用該所產生的認證資訊及第二筆資訊，執行該記錄裝置與該記錄媒體之間的相互認證。

2.如申請專利範圍第1項之方法，進一步包括下列步驟：

藉使用得自於該記錄媒體之加密密鑰對該第一筆資訊進行加密而產生該認證資訊。

3.一種用於對記錄於記錄媒體上複製的內容進行再生之再生裝置與該記錄媒體之間的相互認證方法，該記錄媒體具有算術處理功能，該方法包括下列步驟：

至少將取決於該記錄媒體的第一筆資訊儲存於該記錄媒體中，而亦取決於該記錄媒體的第二筆資訊將於與該再生裝置執行相互認證時，與該再生裝置共享；及

由該再生裝置產生認證資訊，其用於依據得自於該記錄媒體之第一筆資訊而與該記錄媒體進行相互認證，並使用該所產生的認證資訊及第二筆資訊，執行該再生裝置與該記錄媒體之間的相互認證。

4.如申請專利範圍第3項之方法，進一步包括下列步驟：

藉使用得自於該記錄媒體之加密密

鑰對該第一筆資訊進行加密而產生該認證資訊。

5.一種記錄裝置，用以記錄一記錄媒體上之複製的內容，同時對於將記錄於該記錄媒體上之複製的內容數量加以限制，該裝置包括：

產生認證資訊的產生裝置，其用於與該記錄媒體相互認證，並將依據得自於該記錄媒體並依據該記錄媒體的第一筆資訊，而與該記錄媒體共享；及

相互認證裝置，其用於使用該產生裝置所產生的認證資訊，執行與該記錄媒體相互認證。

6.如申請專利範圍第5項之裝置，其中該產生裝置藉對使用得自於該記錄媒體之加密密鑰對該第一筆資訊進行加密而產生該認證資訊。

7.一種再生裝置，用以對記錄於一記錄媒體上之複製的內容進行再生，同時對於將記錄於該記錄媒體上之複製的內容數量加以限制，該裝置包括：

產生認證資訊的產生裝置，其用於與該記錄媒體相互認證，並將依據得自於該記錄媒體並依據該記錄媒體的第一筆資訊，而與該記錄媒體共享；及

相互認證裝置，其用於使用該產生裝置所產生的認證資訊，執行與該記錄媒體相互認證。

8.如申請專利範圍第7項之裝置，其中該產生裝置藉對使用得自於該記錄媒體之加密密鑰對該第一筆資訊進行加密而產生該認證資訊。

9.一種具有算術處理功能的記錄媒體，包括：

儲存裝置，用於預先儲存對該記錄媒體而言是唯一的第一筆資訊，以及第二筆資訊將與一記錄裝置及一再生裝置所共享，前者用於記錄該記錄媒體上複製的內容，後者則於執行記錄媒體、記錄裝置及再生裝置之間的相互認證時依據該記錄媒體再生該複製的內容；及

相互認證裝置，使用依據第一筆資訊由該記錄裝置及該再生裝置所產生之認證資訊，以及第二筆資訊來執行該記錄媒體和該記錄裝置之間，以及該記錄媒體和該再生裝置之間的相互認證。

圖式簡單說明：

圖1是一方塊圖，顯示一音樂內容使用管理系統(LCM，許可的相容模組)的設計範例，其使用一內容管理技術，限制複製的內容數量，依據本發明一具體實施例，該複製內容可記錄於一記錄媒體上；

圖2顯示一記憶體區的映圖範例；

圖3是一方塊圖，顯示記錄／再生裝置(PD，個人裝置)的內部設計範例；

圖4A至4C是三種不同記錄媒體特性的說明檢視；

圖5是一方塊圖，顯示一媒體介面(I/F)的內部設計範例；

圖6是登入(chick-in)後，記錄媒體上所記錄內容的說明檢視；

圖7A至7C顯示一許可的相容模組(LCM)之機密區中所儲存之訪客登錄的儲存範例；

圖8A及8B為相互認證方法輪廓的說明檢視；

圖9是一登入／登出(check-out)程序的說明流程圖；

圖10是當記錄媒體類型為第2級時，登出程序的說明圖；

圖11是當記錄媒體類型為第2級時，再生程序的說明圖；

圖 12 是當記錄媒體類型為第 2 級時，登入程序的說明圖；

圖 13 是當記錄媒體類型為第 2 級時，另一登出程序的說明圖；

圖 14 是當記錄媒體類型為第 2 級時，另一再生程序的說明圖；

圖 15 是當記錄媒體類型為第 0 級時，登出程序的說明圖；

圖 16 是當記錄媒體類型為第 0 級時，再生程序的說明圖；

圖 17 是當記錄媒體類型為第 0 級

時，登入程序的說明圖；

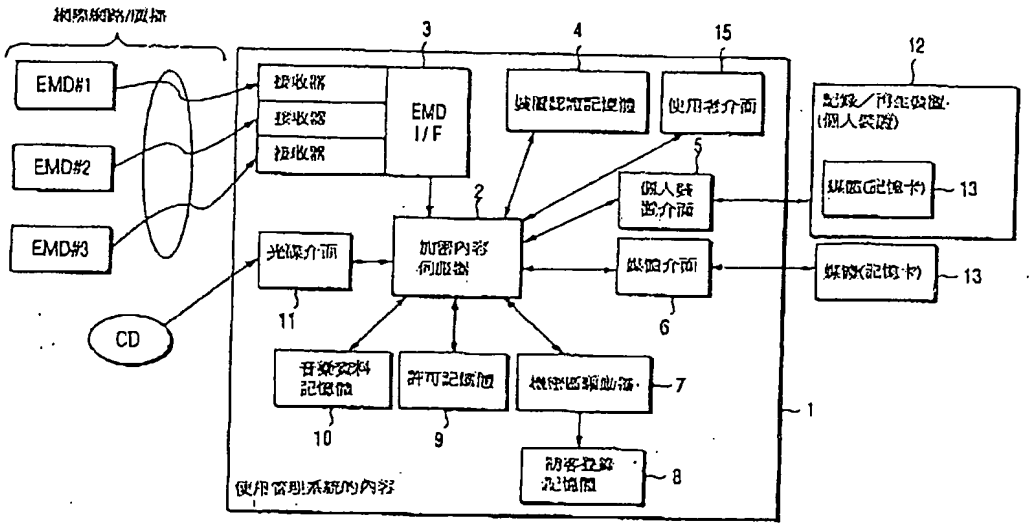
圖 18 是當記錄媒體類型為第 0 級時，另一登出程序的說明圖；

圖 19 是當記錄媒體類型為第 0 級時，另一再生程序的說明圖；

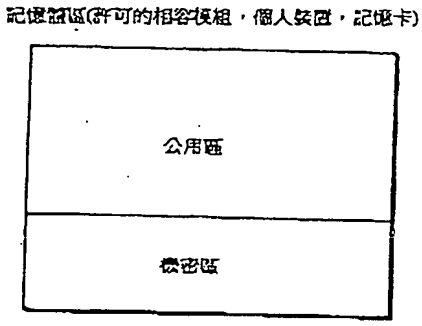
圖 20 是當記錄媒體類型為第 0 級時，另一登入程序的說明圖；

圖 21 是相互認證程序(AKE)的操作程序解說圖；

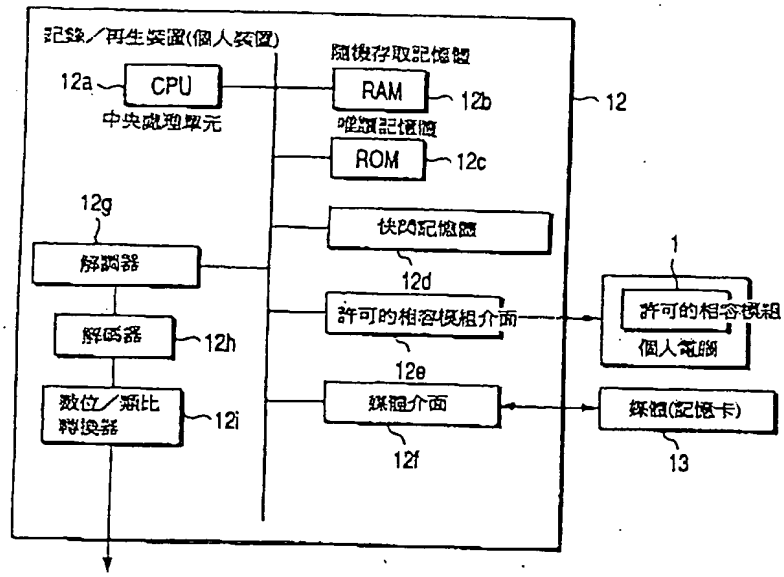
圖 22 是相互認證程序(AKE)的另一操作程序解說圖。



第 1 圖

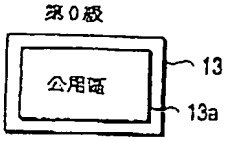


第 2 圖

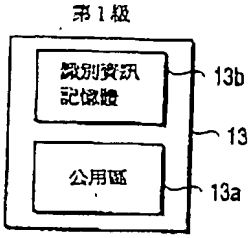


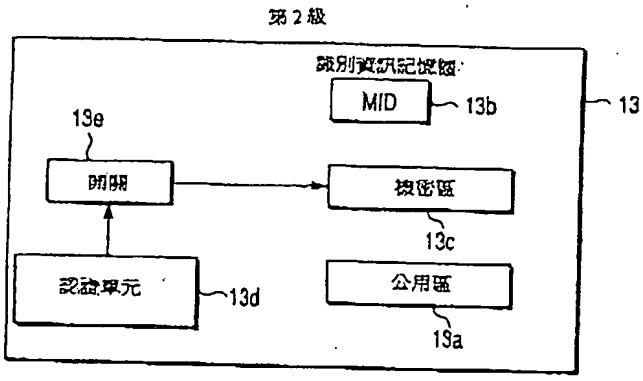
第 3 圖

第 4A 圖

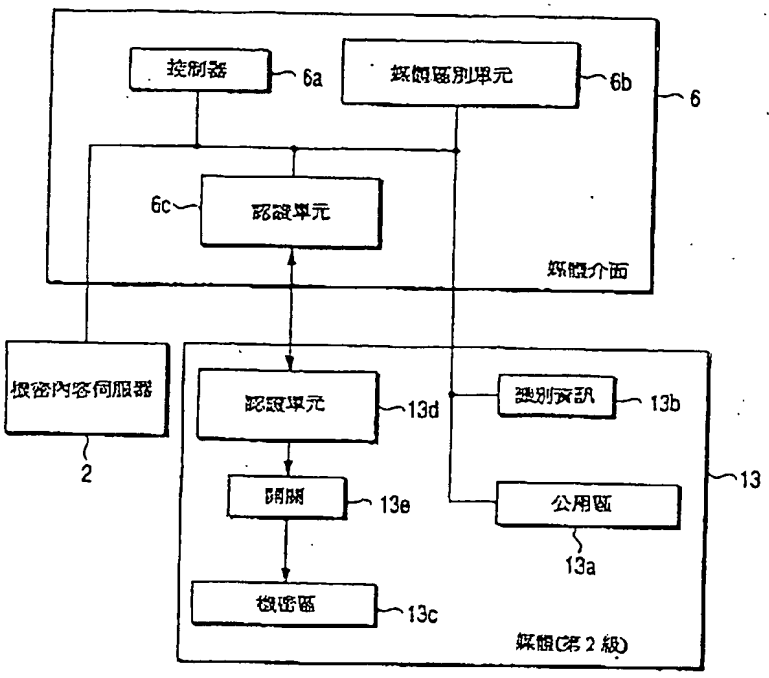


第 4B 圖

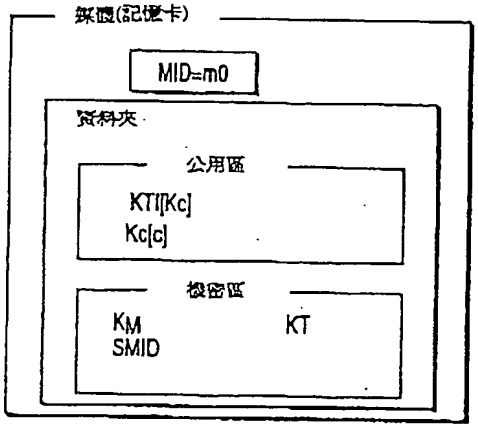




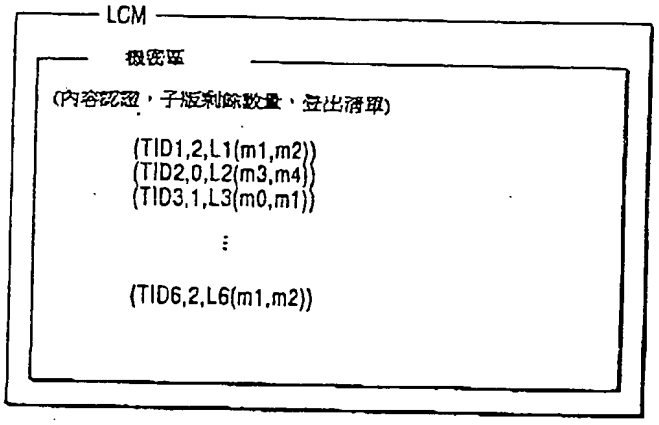
第 4C 圖



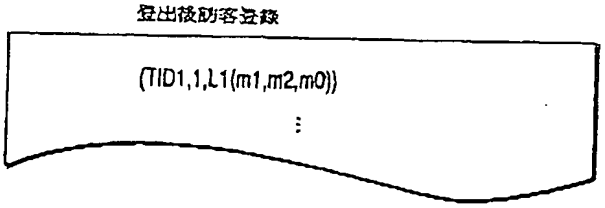
第 5 圖



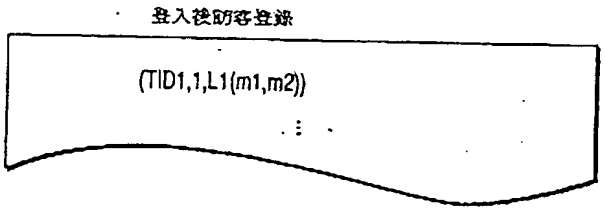
第 6 圖



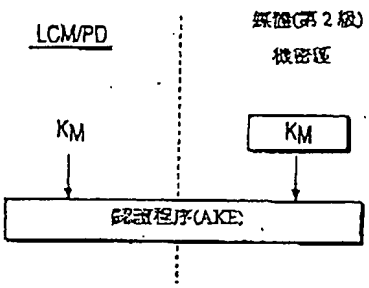
第 7A 圖



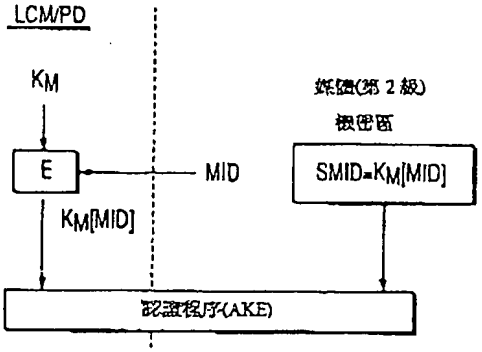
第 7B 圖



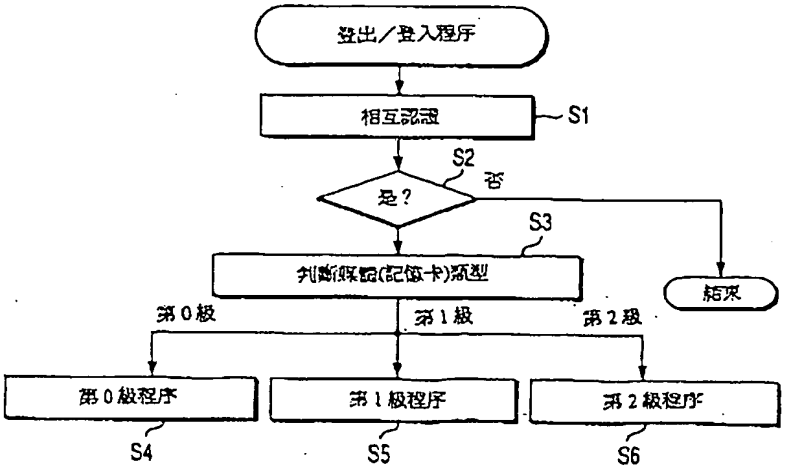
第 7C 圖



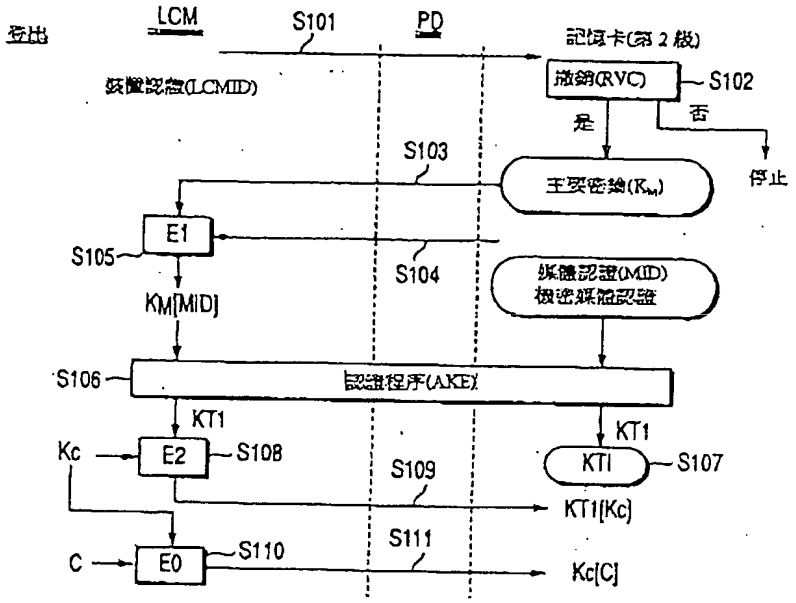
第 8A 圖



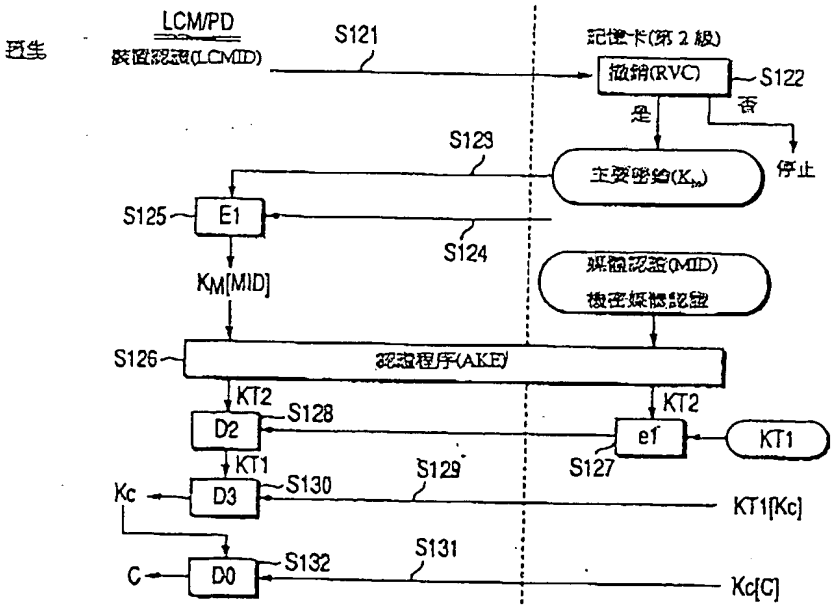
第 8B 圖



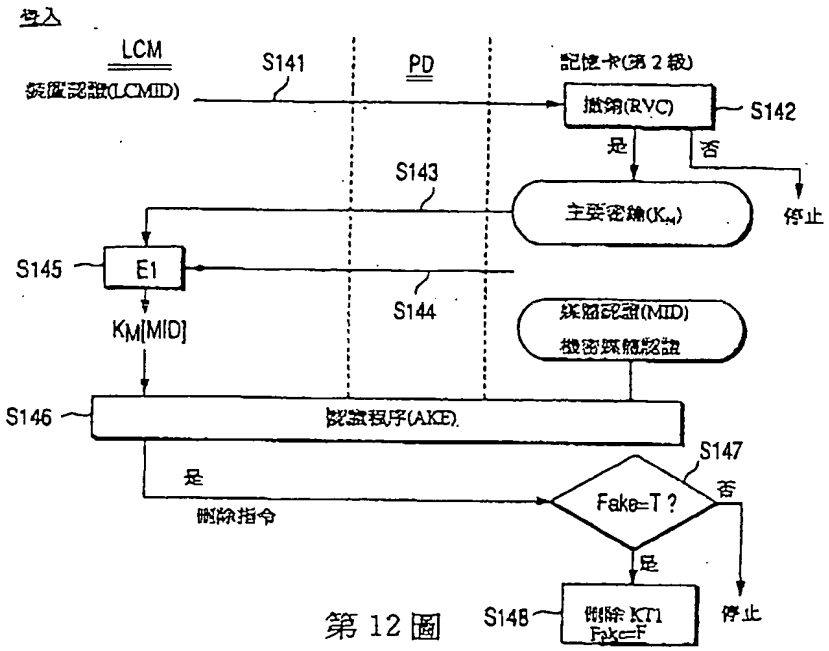
第 9 圖



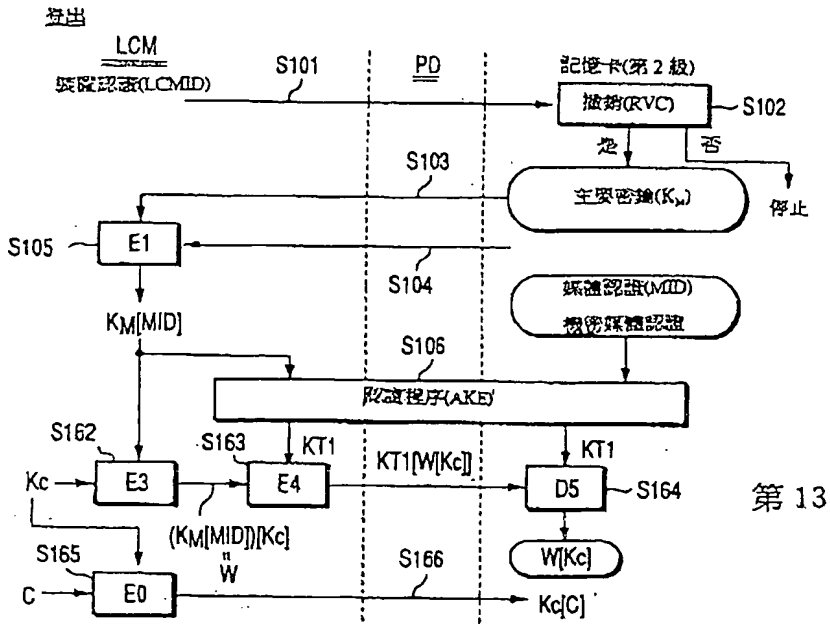
第 10 圖



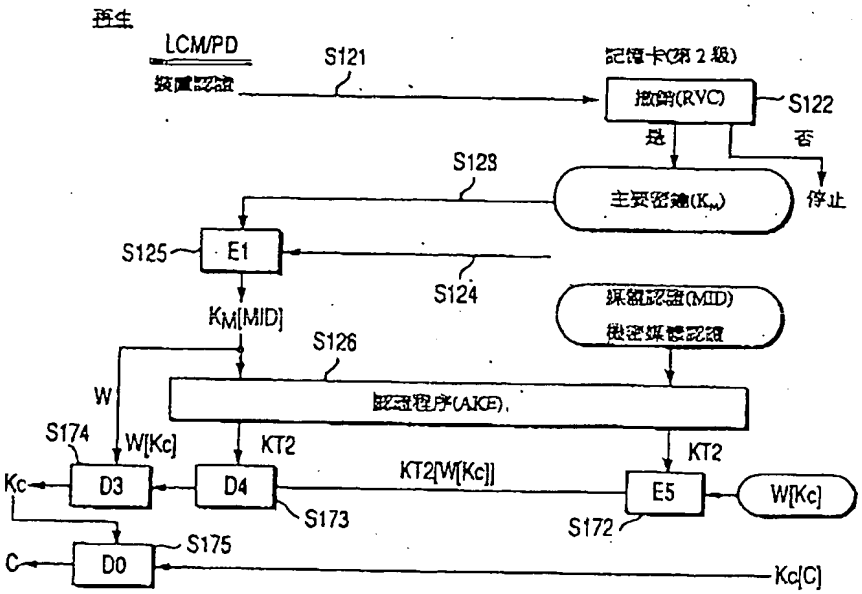
第 11 圖



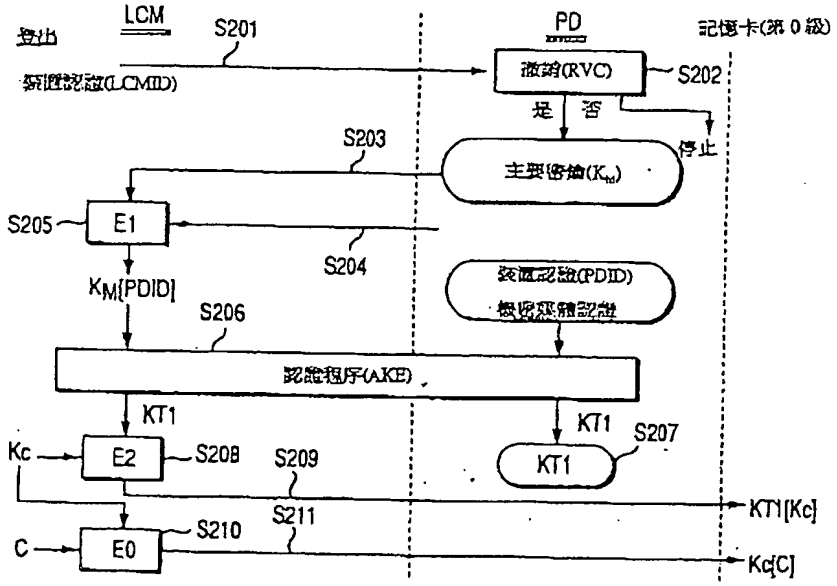
第 12 圖



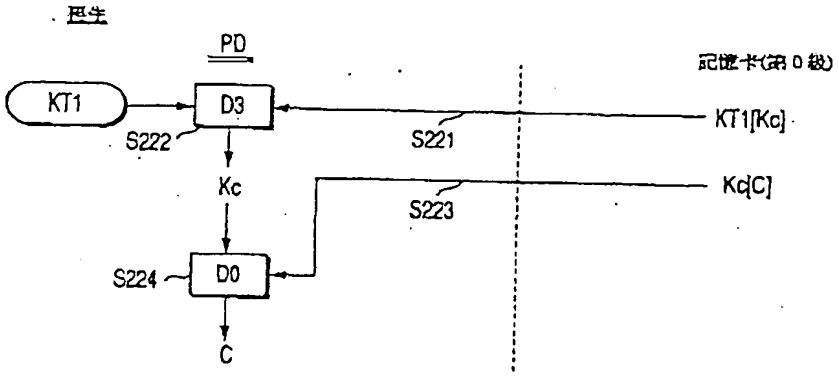
第 13 圖



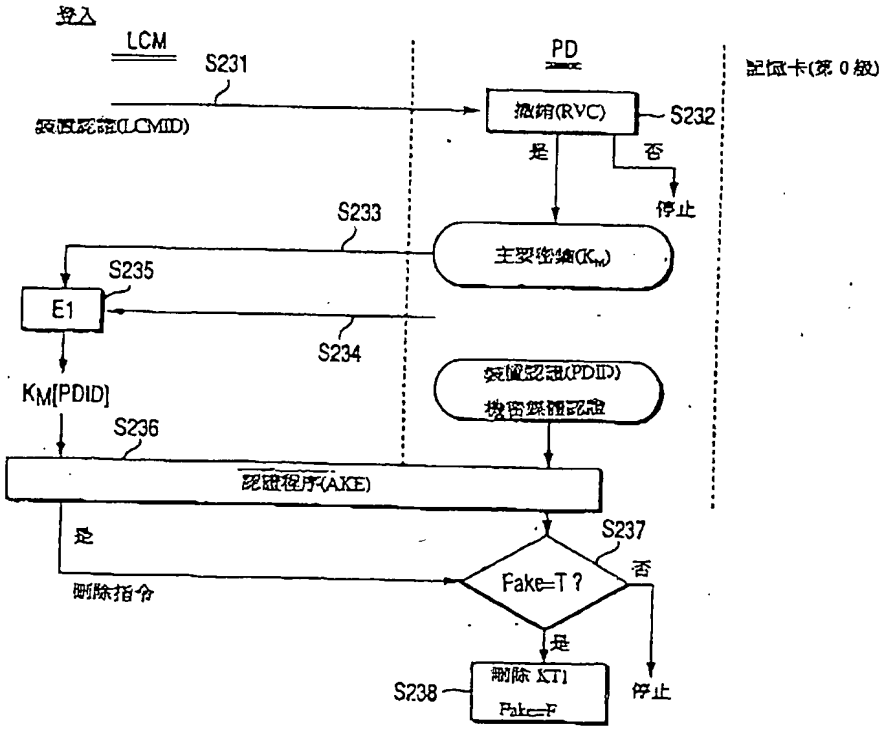
第 14 圖



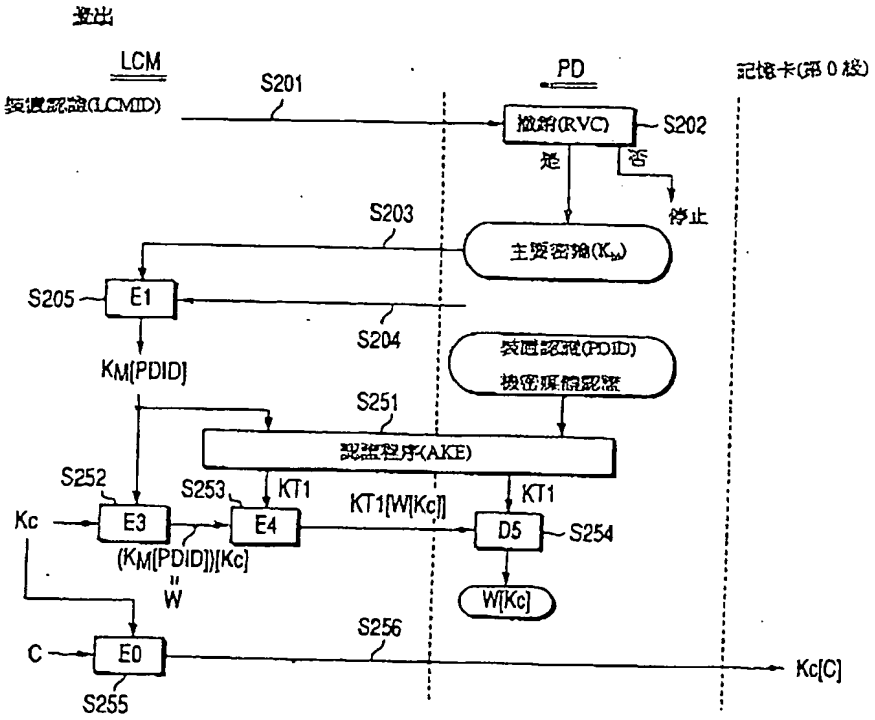
第 15 圖



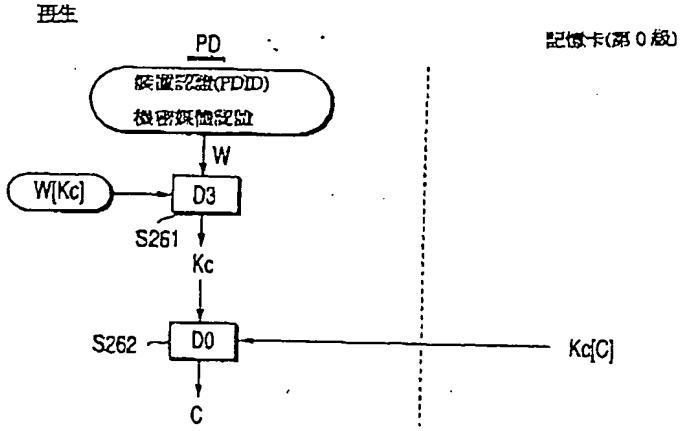
第 16 圖



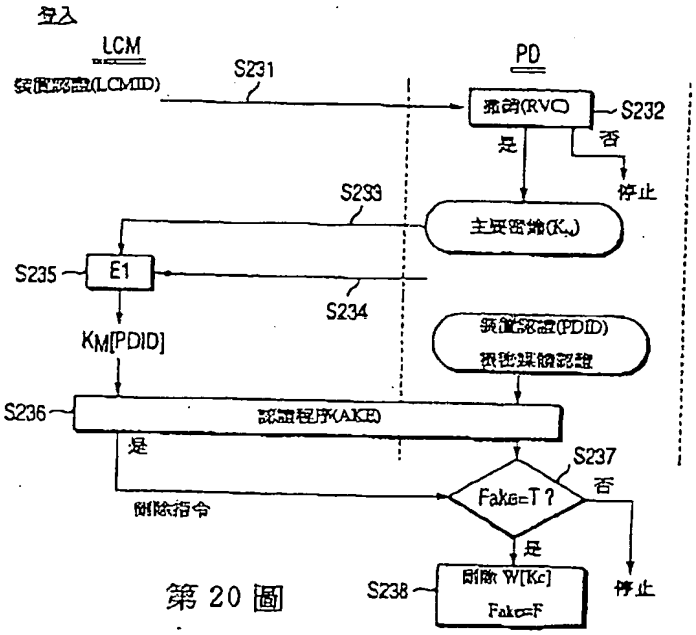
第 17 圖



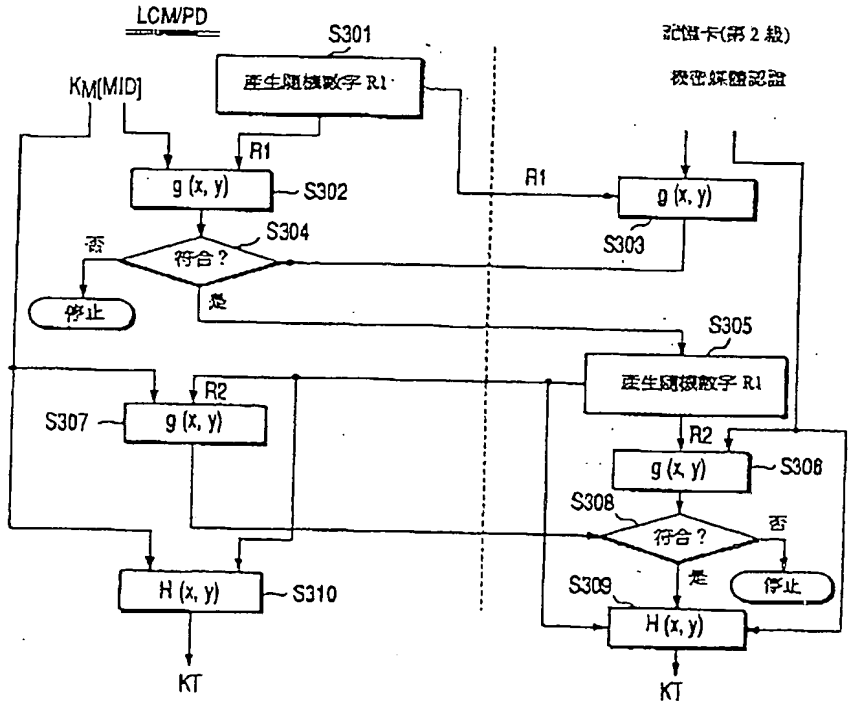
第 18 圖



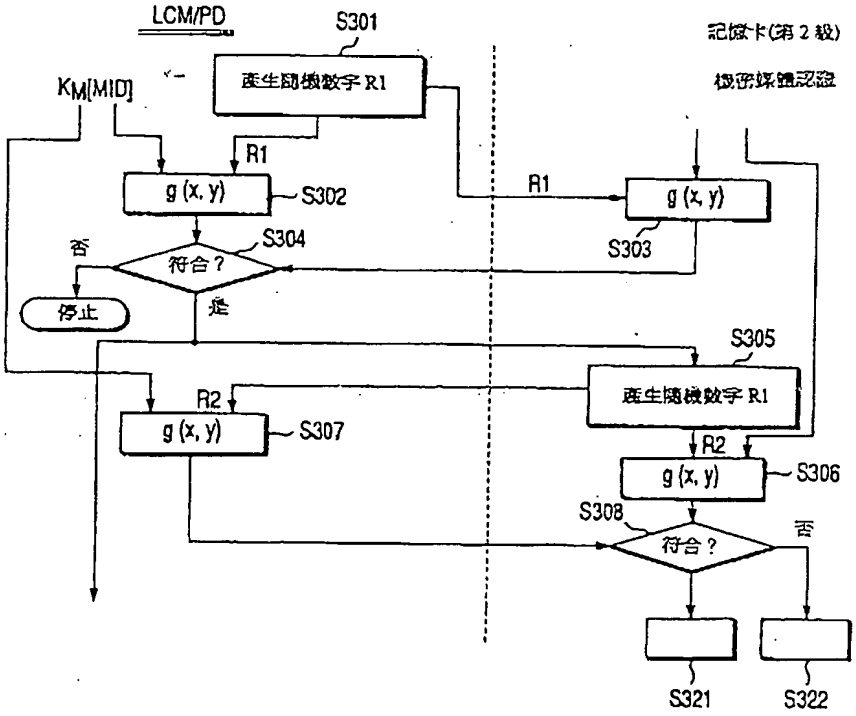
第 19 圖



第 20 圖



第 21 圖



第 22 圖